Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities

January 2001

V. CRITICAL INFRASTRUCTURE PROTECTION R&D

V. CRITICAL INFRASTRUCTURE PROTECTION R&D

Since the publication of Version 1.0 of the *National Plan for Information Systems Protection* in January 2000, an aggressive and fruitful investigation of the need for and solutions to CIP R&D issues has taken place under the auspices of the CIP R&D Inter-Agency Working Group (IWG). Each subgroup has aggressively addressed areas of concern and posed solutions. A description of these, and of the concept for the Institute for Information Infrastructure Protection (I3P) follows.

Information and Communication

The information and communications (I&C) sector of the nation's critical infrastructures generates more revenue than most nations produce. The potential of the new technologies has enabled the U.S., far more than any other nation, to reshape its governmental and commercial processes. We have led the world into the Information Age, and in so doing have become critically dependent on information technologies to conduct national and international commerce, governmental functions, and military operations. These technologies enable us to keep our economy competitive, our government efficient, and our people safe. Thus, as the Honorable Neal Lane recently testified before a joint meeting of two Subcommittees of the House Committee on Armed Services, ensuring the robust and reliable operation of our critical infrastructures " is truly a national challenge - one that goes way beyond the traditional bounds of national security as our economic security, competitiveness, and our way of life rest upon the continuous and assured availability of the services provided by our infrastructures..."[1]

Implementing I&C infrastructure protection through various means such as a viable R&D effort is neither an entirely public nor an entirely private responsibility. The risks to the infrastructure are common to government, business, and citizen alike. Reducing those risks will require coordinated effort within and between the private and public sectors. The need for I&C CIP creates a zone of shared responsibility and cooperation among industry, government, and academia. If we are to retain and build upon the competitive edge information technology has given us, we need to work together on CIP R&D and in other pursuits to substantially improve the trustworthiness of our information systems and networks.

Major Efforts Underway

For FY 2001, nine Federal departments in the President's budget submission to Congress requested funds for 84 ongoing I&C CIP R&D programs. Some of these activities, however, are funded out of program base in other programs and therefore do not appear as separate line items in the budget. The research areas or topics these programs address run the gamut from public key infrastructure and Internet security to mobile agents and advanced authentication systems. As part of the strategic oversight of these programs, the CIP R&D interagency working group has worked with other interagency, Government/industry, and industry groups in sponsoring several Government/private sector workshops. Many of these programs are cooperative endeavors or joint efforts between and among different departments, and a few are joint efforts between Government and universities. For example, the DOD is sponsoring research at universities in its *University Research Initiatives - Centers of Excellence* program in a well-established method of focused research programs on a wide range of topics. Under this initiative, a broad area announcement was issued for CIP and information assurance research proposals

[1] Statement of Dr. Neal Lane, Assistant to the President for Science and Technology and Director of the Office of Science and Technology Policy, before a joint hearing of the Readiness Subcommittee and the Research and Development Subcommittee of the U.S. House of Representatives Committee on Armed Services, March 8, 2000.

from universities, and the research will be funded in FY 2001after review and selection of the proposals on a competitive basis.

Major Challenges in the I&C Area

Gaps and shortfalls have been identified after mapping the currently funded R&D against identified vulnerabilities and shortcomings in the U.S. I&C infrastructure. Those gaps and shortfalls fall into four primary thrust areas:

- Threat/Vulnerability/Risk Assessments - focusing on threat, vulnerability, and risk assessments of the I&C critical infrastructure, to include modeling and simulation programs, metrics, and test beds;
- System Protection - cyber protection of individual systems, to include programs such as encryption, public key infrastructures, network security products, reliability and security of computing systems, robust I&C control systems, and secure supervisory control and data acquisition (SCADA) systems;
- Intrusion Monitoring and Response - technologies to detect and provide immediate responses to intrusions or infrastructure attacks, to include such programs as network intrusion detection, information assurance technologies, mobile code and agents, network alarm systems, forensic tools for electronic media, and network defensive technologies; and
- Recovery and Reconstitution - those technologies required to reconstitute and restore the I&C critical infrastructure in the aftermath of disruptions, to include such programs as risk management studies and tools, system survivability technologies, and consequence analysis tools and supporting technologies.

Banking and Finance

While there are some vulnerabilities and threats unique to the banking and finance sector, the sector's critical infrastructure exposure is essentially an overlay on the I&C infrastructure. One issue facing the sector is that there has been little R&D of any kind done in this community. The only work that fits the traditional definition of R&D would be the development of new derivatives and financial forecasting tools.

In order to address the new and expanding threats from foreign nation states, criminal enterprises and terrorists, the community has sponsored, with the support of the Treasury Department, a number of initiatives. In addition to the Information Sharing and Vulnerability Assessment Center (FS/ISAC) there is a R&D working group under Mr. Charles Blauner – J.P. Morgan & Co. This working group has identified what work is being done within the community and vetted the efforts underway within the government and I&C sector.

The major focus of the FY 2001 program is a modeling effort to identify the vulnerabilities in the banking and finance sector critical infrastructure. This activity builds on work of the National Communications System (NCS), which has completed an extensive model of the United States backbone communications network. This object-oriented model is aimed at understanding the properties, vulnerabilities and required remediation for our national communications infrastructure. As mentioned before, almost all banking and financial services travel over some portion of the communications infrastructure. Accordingly, this effort overlays essential services such as funds transfer, clearing houses, stock markets, refunding, etc. in order to identify the inherited vulnerabilities from the communications infrastructure and best remediation approaches. For example, we may know that there is an existing or pending attack against a certain type of switch. Examination of the model will show where the switches are and which essential financial services depend on them, further examination will show the extent of the impact and what alternatives are available. As the sophistication of the tool develops a better understanding of

financial processes, the model will also be able to identify malicious intervention or criminal activity. While this level of sophistication will take time to develop, the simple mapping of financial transaction and funds flow to the communications model will reap tremendous results. This tool brings a number of benefits: identification of potential vulnerabilities; the testing of remediation alternatives to find the best option; and a tool for executive crisis management training and exercises. During an actual crisis or information warfare attack, the extent of impact can be quickly identified and responses evaluated in real time. This effort will serve as a model technology for identifying infrastructure interdependencies with other sectors.

The sector's secondary focus is on the development of the forensic tools need by the United States Secret Service and other law enforcement agencies in combating electronic crimes and attacks on the banking and finance sector critical infrastructure. This work is being done in coordination with efforts at the Justice Department, but focuses on the specific nature of electronic financial crimes.

The total budget request for fiscal year 2001 was $4 million, which will only provide "seed money" for these efforts. The task of examining the vulnerabilities and interdependencies of the entire banking and finance sector is so overwhelming that there is no meaningful alternative to the efforts to develop mature modeling tools. Once we have the resources and develop the modeling tools, then we can start the R&D efforts to develop remediation for the vulnerabilities that will be identified by the modeling efforts.

Energy

Our nation's energy infrastructure—composed of increasingly interdependent industries that produce and distribute electric power, oil, and natural gas— is undergoing rapid and dramatic changes. Advances in information technology, an increased reliance on electronic commerce, restructuring and deregulation initiatives, and other market forces are motivating much of these changes. The purpose of the energy subgroup is to develop an agenda for a R&D program that will address a wide range of needs related to protecting this critical energy infrastructure. Applicable R&D encompasses the physical and cyber components of the electric power, oil, and gas infrastructures, the interdependencies among those components, and the interdependencies with the other critical national infrastructures. The energy R&D program is aimed at developing cost-effective technologies and capabilities (e.g., databases, methodologies, tools) that can be used to achieve several goals:

- Increase our understanding of physical and cyber disruptions (natural, accidental, deliberate) to the energy infrastructure that could result in cascading or widespread regional outages;
- Develop energy infrastructure assurance "best practices" through vulnerability and risk assessments; and
- Protect against, mitigate the impacts of, and improve our ability to recover from disruptive incidents within the energy infrastructure.

Major Efforts Underway

The R&D agenda consists of two primary thrust areas: Analysis and Risk Management, and Protection and Mitigation Technologies. Specific topical areas include:

- Infrastructure Interdependencies - Development of methodologies and tools for characterizing and analyzing interdependencies among the energy infrastructures and with other critical infrastructures. This capability will help DOE and others within the energy sector identify critical system nodes and assess the technical, economic, and national security implications of energy technology and policy decisions designed to ensure the security of our nation's interdependent energy systems.

- Vulnerability Assessment - Focus on collaboration with the energy sector to conduct physical and cyber vulnerability assessments that identify infrastructure vulnerabilities, raise awareness about these vulnerabilities, and enable the development of guidelines and best practices for industry to use in limiting vulnerabilities.

- Scale and Complexity Analysis - Research on the fundamental operational characteristics of large-scale, complex, nonlinear energy infrastructures. Development of technologies and capabilities that focus on stability, countermeasures, reduction of complexity, the effects of uncertainty, and behavior.

- Consequence Analysis and Management - Development of data, methodologies, and tools for evaluating the public health and safety, national security, and economic consequences of disruptions to energy infrastructures and the processes needed to assist in restoration and reconstitution following such disruptions.

- Risk Management - Development of risk management methodologies and tools to assist decision makers in quantifying system risks and in planning and implementing critical infrastructure protection strategies.

- Policy Effects and Institutional Barriers - Examination of the barriers between government and industry stakeholders in sharing CIP-related information (e.g., threat and vulnerability information) and identification and implementation of solutions to barriers that may inhibit our ability to protect our nation's critical infrastructures.

- Real-time Control Mechanism Technologies - Identification of vulnerabilities inherent in real-time energy control systems and development of technologies for protecting against disruption to, unauthorized control of, or intrusion into these systems.

- Integrated Multisensor and Warning Technologies - Improvement of existing integrated systems and/or development of new ones to warn of attacks and impending failures at critical nodes. Focus on anomaly detection and failure warning technologies.

Major Challenges in the Energy Area

R&D task areas are structured to complement and reinforce each other and related efforts. Capitalizing on the links and synergies across the initiatives to meet requirements is a major technical and programmatic challenge. Additional challenges in the energy sector which complicate the R&D picture include:

- Inadequate information to determine susceptibility to disruption of the energy infrastructure;
- Lack of a coordinated process to collect and distribute threat information;
- Inadequate response and recovery procedures and technology;
- Interdependence of energy infrastructure and other infrastructures;
- Increasing system interconnectedness and complexity of the energy system;
- Increasing reliance on real-time system control;
- Gaps in physical protection for energy infrastructure facilities;
- Limited cyber security for SCADA systems;
- Inadequate protection of energy-related information;
- Reliance on unique, hard to procure equipment and materials;
- Susceptibility to cascading failures; and
- Reliance on rapid access to accurate information.

Conclusion

Coordination and partnerships among agencies and the private sector are of paramount importance. Identifying and developing mechanisms to transfer the technologies, capabilities and best practices developed through this program to industry and public organizations at the Federal, state, and local levels are key to the success of the program and to protection of our nation's critical infrastructure.

Transportation

The Transportation Subgroup of the National Science and Technology Council (NSTC), Committee on Technology, Interagency Working Group on Critical Infrastructure Protection (CIP IWG) R&D includes representatives from a number of DOT offices, as well as several Federal agencies. Incorporating relevant projects and proposals from these organizations, the subgroup formulated the Interagency Transportation Infrastructure Assurance (TIA) R&D plan. This plan provides a coordinated Federal government response to the PCCIP (1997), White House Commission on Aviation Safety and Security (1997), the DOT Surface Transportation Vulnerability Assessment (1999), the National Research Council report, *Improving Surface Transportation Security: A Research and Development Strategy* (1999), and related Presidential Decision Directives (e.g., PDD-62, PDD-63, PDD-67). These activities and initiatives are deemed essential to protecting the nation's transportation infrastructure, operators, and users against future acts of terrorism and crime and will enable the transportation system to adapt rapidly to natural or intentional disruptions. Critical transportation infrastructure elements include: aviation, space transportation, highways, mass transit, pipelines, rail, waterborne shipping, intermodal connections, and interfaces with other transportation-dependent infrastructures, such as energy and telecommunications.

The goal of the Interagency TIA R&D Plan is to develop a comprehensive approach to assessing threats to the security of the nation's transportation system and to preparing R&D projects that provide integrated security solutions (e.g., technologies, procedures) tailored to these threats. It addresses the:

- Physical security of transportation modes and intermodal connections (e.g., roads, railroad lines, bridges, tunnels, terminals, locks and dams, piers, etc.);
- Security of vital communications, navigation and information systems and networks (e.g., GPS);
- Susceptibility of transportation operators and users to weapons of mass destruction (WMD); and
- Development and dissemination of information about system threats, vulnerabilities and best practices to transportation system developers, operators and users.

Major Efforts Underway

Traditionally, aviation, through the Federal Aviation Administration, has conducted the bulk of transportation CIP R&D. This trend continues today as aviation assumes approximately 79 percent of on-going transportation CIP R&D in the area of aviation security (FY 2001). Aviation security projects include:

- Explosives and weapons detection;
- Airport security technology integration;
- Airport security human factors; and
- Aircraft hardening.

Other current major transportation CIP R&D efforts include:

- Analysis on GPS vulnerabilities;
- Intelligence and security risk assessments;
- Threat assessment/information dissemination;
- Infrastructure assurance training/awareness;
- Vulnerability and risk analysis of transportation systems;
- Chemical/biological agent detection;
- Intermodal terminal security at major transportation nodes;
- Human factors analysis for transportation systems;
- Research on operational methods for improving performance of transportation systems;
- A pilot study to determine the ambient environmental background, using high efficiency particulate arresting (HEPA) filters, to establish a "clean air" baseline in certain public areas of transportation facilities in the event of chemical or biological attack and subsequent decontamination clean-up efforts;
- An on-going vulnerability assessment of the interstate roadway system, rail lines, and bridges to determine their susceptibility to disruption by conventional or other means, and what ancillary effects might occur to the national surface infrastructure system and regional or national economies; and
- An analysis to determine current DOT information cyber security gaps in computer networks vital to transportation cyber information systems and subsequently conduct R&D to remedy current cyber information security gaps.

Major Challenges to the Transportation Sector

Responsibility for assuring the safety and the security of the nation's transportation infrastructure and its continued operations is scattered among thousands of private companies and government agencies at all levels (from local to Federal). This decentralized approach to transportation has caused gaps in transportation system security, especially in areas where both responsibility and resources are divided or uncertain. A second major challenge involves information control of vulnerability assessments. The crux of the challenge involves the following questions: How can vulnerability assessments remain classified in such a manner to not allow inappropriate Freedom of Information Act distribution, yet allow private companies to obtain the needed information? Additionally, many vulnerability assessments could involve the gathering of sensitive, proprietary information, which, if provided to competitors, would be damaging to the participating private company. How should this information be protected? Many private companies fear that vulnerability assessments of their operations could open the door for tort liability. Although these questions have yet to be fully resolved, efforts are underway to address these concerns.

Conclusion

Aviation has a strong history of robust R&D efforts with regard to transportation infrastructure assurance and security. This will continue. But, because of surface transportation's importance and vulnerability, as highlighted by several recent studies and high-profile incidents, improving surface transportation security is essential given emerging 21st Century threats – cyber terrorism and chemical and biological weapons. The interagency development of the TIA R&D plan addresses and coordinates these challenging tasks of protecting our nation's transportation infrastructure from terrorist threats. The plan's next stage will include heightened involvement of private industry in developing and honing transportation infrastructure assurance R&D.

Vital Services

The Vital Human Services (VHS) sector includes three of the critical infrastructures: water supply, emergency services, and government services. The three VHS infrastructures differ from other critical infrastructures in that they are focused largely at the state and local level and are largely governmental responsibilities. In spite of these differences, the VHS infrastructures face similar problems and vulnerabilities in communities across the country. This section of the report highlights the research and development efforts underway in the water supply and emergency services sectors.

The water supply sector CIP effort is primarily focused on the 330 large water supply systems, which serve more than 100,000 people. The U.S. EPA, as lead agency for the water supply sector, is working in cooperation with various associations, especially the American Water Works Association (AWWA) and the Association of Metropolitan Water Agencies (AMWA). Through these partnerships, EPA hopes to raise awareness of water sector vulnerabilities, encourage information sharing, and develop remediation protocols for the vulnerabilities that are discovered. The initial research effort is small and is focused on developing a vulnerability assessment methodology. Additional Federal agencies including the Department of HHS and FEMA also assist with efforts in the water supply sector.

HHS has requested funding to focus on emergency services infrastructures. Efforts include identifying key areas of interdependence between hospital and health care response and communications and transportation infrastructures and working with hospitals and related emergency services to identify operational vulnerabilities and to determine ways to mitigate those vulnerabilities.

Major Efforts Underway

In FY 2000, EPA entered into an inter-agency agreement with the Department of Energy's (DOE) Sandia National Laboratories to develop a vulnerability assessment methodology for the water supply sector. This methodology is an extension of the methodology developed for the Federal dam community. The Federal dam community includes the Corps of Engineers, Bureau of Reclamation, Bonneville Power Authority, and TVA. The AWWA–Research Foundation, a private not-for-profit organization, which sponsors research for the drinking water industry, has also entered into a contract with Sandia to further support this vital work. Funds requested by HHS are also expected to assist in this effort. In the fall of 2000, a workshop with six to eight representatives of large water utilities outlined a methodological approach. This effort will extend into FY 2001 and, if funded, the effort will be expanded to include field-testing and training for users.

In August 2000, EPA held a joint meeting on the water supply infrastructure with DOE at their Argonne National Laboratory. Most of the major Federal water agencies and approximately 30 water utilities were represented. Meeting attendees reached an agreement on the approach and the priorities for water supply sector research. The recommendations from that meeting will be available shortly.

For FY 2001, funds were requested in the President's budget submission and appropriated by Congress to initiate a more robust water sector CIP program. The direction from OMB to the EPA is as follows:

> "Through partnerships with AMWA and AWWA, EPA will work with water utilities undertaking measures to safeguard water supplies from terrorist and seditious acts. EPA will also implement an assessment of the vulnerability and methods to reduce vulnerability of the drinking water supply to terrorists acts."

Other areas of interest include remediation measures, threat analysis and communications techniques, methods to identify and characterize chemical and biological agents, and a university or industry-based center of excellence in risk assessment and risk reduction. Specific efforts are underway, in cooperation with FBI, to develop an ISAC for the water supply sector to facilitate the exchange of threat and vulnerability information.

FEMA is also leading an effort to produce valid and verified databases of water distribution systems and to develop assessment tools for evaluating the threat to public health and safety posed by the introduction of a biological or chemical agent into a water system. Two prototype databases and assessment tools will be developed covering: broad area populations at risk (statewide) and local area populations at risk (citywide). The broad area prototype will allow the user to track an agent, under variable flow conditions, from the point of introduction to downstream water supply intakes and will determine the concentration and decay rate of an agent as it is dispersed within the water source. The local area prototype will allow the user to model the flow and concentration of an agent within a city or municipal water system, will assess the effects of water treatment on the agent, and will model the flow and concentration of an agent through the water distribution system.

The funds requested by HHS will focus on three of the VHS sector's high priority research and development issues identified by the interagency CICG. First is the previously mentioned effort to develop a vulnerability assessment methodology for the water supply sector. Emergency services infrastructure issues include studying critical interdependencies between hospital and health care response systems and the communications, essential transportation, public safety, and emergency medical systems. This effort will look at how threats or damage to communications and transportation systems may affect the response capabilities of the hospital and health care community. A related effort will look at protection of hospital infrastructures. This effort will focus on critical hospital operations in response to a chemical or biological incident including decontamination, preventing cross-contamination, hospital capacity, etc.

Major Challenges in the VHS R&D Area

On-going water sector research is a small effort and leaves gaps and shortfalls in addressing identified vulnerabilities and shortcomings relative to U.S. water supplies. EPA is coordinating its efforts closely with other Federal agencies and the private sector to identify the highest priorities and to work jointly to develop solutions to vulnerabilities and shortcomings.

Gaps and shortfalls exist in four major areas:

- Threat/Vulnerability/Risk Assessments – Focusing on threat, vulnerability, and risk assessment of the water supply sector critical infrastructure to include methodologies, benchmarks, field-testing and analysis and communication of results.

- Supervisory Control and Data Acquisition (SCADA) Systems – Application of information assurance techniques to water supply SCADA systems and development of appropriate, cost-effective protocols. Since the SCADA systems used in water utilities are similar to those used in the gas, oil, and electric power sectors, this work will rely heavily on efforts being conducted by DOE.

- Identify and Characterize Biological and Chemical Agents – In conjunction with CDC and other agencies, identify and characterize the behavior of chemical and biological agents in water. Determine the effects of water treatment on these agents and characterize the actual risks posed by these agents to the nation's water supply.

- Center of Excellence for Risk Assessment of Water Supplies – Establish a center of excellence to support communities in conducting vulnerability and risk assessments and in making decisions regarding water supply assurance.

Conclusion

The cooperation of the water supply industry is essential in developing realistic research needs and in developing the tools that they need to evaluate and correct vulnerabilities. EPA has succeeded this year in establishing a good relationship with the major water association and has an agreement with them as to future priorities.

Interdependencies

The economy and national security of the United States are becoming increasingly reliant on a spectrum of highly interdependent U.S. and international infrastructures. This trend has accelerated over the last ten years with the proliferation of information technology and concomitant infrastructures, and shows no signs of abating.

This development is relatively recent: while the U.S. economy has long depended on several critical infrastructures, the coupling among them had historically been rather loose. However, during the past few years, important technological, economic, and regulatory changes have dramatically altered the relationships among infrastructures. At the same time as the IT revolution led to substantially more interconnected infrastructures with generally greater centralization of control, "just-in-time" business practices have reduced margins for error in infrastructure support. Deregulation and growth of competition in key infrastructures has eroded spare infrastructure capacity that served as a useful "shock absorber" in key infrastructures. Furthermore, mergers among infrastructure providers have led to further pressures to reduce spare infrastructure capacity as management has sought to wring "excess" costs out of merged companies to realize savings. Any one of these trends would be a cause for uneasiness. The collision of all four has no precedent in American economic history. While important steps have been taken in individual infrastructures, the issue of interdependent and cascading effects among infrastructures has received almost no attention. This situation is starting to change, as the government launches activities designed to yield a greater understanding of the nature and implications of these infrastructure connections.

Major Efforts Underway

Several efforts are underway to try to tackle the difficult issues of interdependencies. These include efforts to learn about the secure operation of complex interactive networks/systems, and furthering the understanding of the dynamics of complex interactive networks/systems; technology development and vulnerability analysis capability R&D, aimed at analyzing national and defense infrastructures and their critical interdependencies; efforts to develop an easy-to-use, deployable state-of-the-art hazard and consequence prediction, digital databases, and a Geographic Information System (GIS), within a Graphical User Interface (GUI); collaborative work between the Disaster Research Center at the University of Delaware and the Research Center for Disaster Reduction Systems, a unit within the Disaster Prevention Research Institute at Kyoto University in Japan to better understand various aspects of damage caused by earthquakes; and interagency efforts to build upon a number of ongoing programs and laboratory testbed facilities.

Major Challenges in the Interdependencies Area

The major efforts underway, as well as those being investigated for the future, are designed to meet the following challenges.

- Building a theoretical framework for understanding and predicting the nature of interdependencies and their effects on the country as a whole.

- Developing the capability to model and simulate in real time the behavior of the nation's interconnected infrastructures by developing an architecture and related enabling technologies that can be used to integrate infrastructure-specific and interdependence databases and analysis tools to study the linkages among the interdependent critical infrastructures, the interdependencies associated with those linkages, their impacts, and their likely causes.

- Developing a set of quantitative metrics for measuring the scale of impacts of interdependency-related disruptions.

- Developing new technologies and techniques to contain, mitigate, and defend against the effects of interdependency-related disruptions, such as escalating, cascading, latent, and cross-infrastructure failures.

- Developing capabilities to adequately and realistically test new methodologies, techniques, and technologies.

- Defining a set of tasks for further work on specific national security policy issues that could be analyzed using these tools and methodologies. This could include, for example, characterizing the potential interdependence implications, from national security and economic perspectives, of current trends within the private sector (e.g., restructuring, deregulation, increased reliance on cyber monitoring and control systems) and their implications for national security; identifying interdependency vulnerabilities in the U.S. economy; and developing metrics for interdependencies.

- Developing the ability to characterize and incorporate new critical infrastructures into the models and methodologies as such infrastructures develop.

Conclusion

Growing interdependencies between critical infrastructures make this set of problems significantly different than those we have faced in the past, and it is what makes them difficult. A significant amount of work is now being done in government, the national labs, academia and private industry to build an understanding of these issues, and tools to solve these problems.

International R&D

Just as our critical infrastructures are inherently international, so too is the global science and technology base that will generate solutions to current and future infrastructure protection vulnerabilities. In general, the U.S. has no monopoly over the relevant technologies. Research and development in the field of information technology is a fully international enterprise today. In fact, it is even difficult to define a "domestic" science and technology base, given the substantial technical contributions made by foreign scientists and engineers within the U.S., by firms in overseas laboratories, and by foreign or multinational firms with U.S. research facilities.

Moreover, the technologies relevant to infrastructure protection are largely unclassified, having been developed in the commercial sector or academia rather than in government or its contractors. Therefore, unless a particular R&D project involves classified material or is identified by its sponsoring U.S. government agency as raising particular sensitivities, it can serve the U.S. national interest to draw on the global science and technology base, and to have the project done by the most qualified technical experts, wherever they may be. Indeed, the U.S. has a history of pursing international science and technology collaboration as a means of stretching development dollars, broadening and deepening the talent pool that can be brought to bear, and building an international constituency for our views. Many of the international science and technology activities now considered to be CIP-related reflect longstanding, and continuing, collaborative efforts of private industry, academia, and government to resolve emerging information technology issues.

The Department of State has undertaken a variety of activities in response to PDD-63, including multilateral negotiations in the European Union, Asia-Pacific Economic Cooperation, Organization for Economic Cooperation and Development and other fora that addressed existing and emerging threats and vulnerabilities to our economic security. The Department of State also led and coordinated bilateral negotiations and meetings with Canada, United Kingdom, and Australia aimed at identifying, developing and facilitating science and technology solutions for CIP.

Multilateral Agenda

EU*:* A United States and European Union Task Force on Science and Technology was established in October 1998 to enhance the security of critical infrastructures by identifying, developing, and facilitating technology and policy solutions to existing and emerging threats and vulnerabilities. The Department of State Co-Chairs this Task Force with a senior EU representative from the Directorate General for Information Society. Over the past year the task force has sponsored a series of workshops and conferences resulting in cooperative exchanges between U.S. technical agencies and EU research organizations; reciprocal exchange of information on cyber security research programs on an annual basis; coordinated research projects; visits and exchanges of scientists; and mutual exchanges of scientific and technological information.

APEC*:* Within the APEC forum, the Department of State succeeded in establishing a dialog on CIP-related telecommunication issues. At the APEC Telecommunications 21 Working Group meeting, in March 2000, the Department worked closely with the Business Facilitation Steering Group (BFSG) to address the relationship and importance of infrastructure protection to e-commerce in each of the economies represented. By working closely with other APEC economies the Department was able to get infrastructure protection added to the APEC Telecommunication Program of Action during the Fourth Ministerial Meeting, held in Cancun, Mexico in 2000. The Department continued to expand the APEC agenda on infrastructure protection science and technology issues and arranged for State sponsorship of a half-day workshop at TEL 22 in October 2000 to develop a forum and advance proposals to facilitate awareness and sharing of information with regard to critical infrastructure science and technology issues in the Asia-Pacific region. At the APEC Telecommunications 22 Working Group meeting in October 2000 the State Department sponsored a proposal, along with Australia and Canada, for development of cyber security training modules to be used by member economies at both undergraduate and graduate level to increase the level of information security awareness and ultimately the protection of critical infrastructure. In the APEC Industrial Science and Technology Working Group, working collaboratively with Department of Commerce, the Department of State has successfully laid the groundwork for introduction of CIP technology cooperation with the aim to identify all relevant research and development in the Asia-Pacific region.

OECD*:* The Department of State initiated a discussion on cyber security issues within the OECD in 2000. At the last meeting of the OECD Working Party on Information Security and Privacy (WPISP) the Department sponsored a presentation highlighting global aspects associated with information security, the economy's dependence on the internet, technical vulnerabilities of the internet, and possible solutions such as the concept of a center for analysis of global incidents, global intrusion detection and identification, research and development, and awareness raising through education and media. This resulted in a discussion among economies and agreement for future work in this area. The Department was also successful in obtaining WPISP agreement in the Work Program for 2001-2002 to examine the present and future state of cyber security including emerging threats and vulnerabilities. The Department's efforts in subsequent meetings of the OECD have resulted in widespread agreement on the importance of cyber security and the role that OECD should take in progressing work in this area including an early review of security guidelines.

Bilateral Agenda

Canada: The Department of State led a bilateral meeting in September 2000 to discuss CIP cooperative efforts at the national and departmental/agency levels and in international fora. There was agreement to establish a CIP R&D Working Group to take stock of current efforts and to identify potential synergies and a short list of areas of further cooperation/joint action. There was also interest expressed in the idea of developing an International Center for Analysis of Global Incidents.

United Kingdom: The Department of State met with representatives from the UK Information Assurance Advisory Council (IAAC) to discuss critical infrastructure protection science and technology issues and to exchange information on respective national and international policies on information assurance. The IAAC, whose membership includes the Cabinet Office, CESG, private industry and academia, has created five working groups to address CIP issues: threat assessment & attack warning, risk assessment and critical dependencies, standards, R&D, education and outreach. The IAAC stressed the importance of industry involvement in addressing the increasing volume of attacks on infrastructure and expressed a desire to work cooperatively with US information sharing and analysis centers.

Australia: The Department of State met on several occasions throughout 2000 to coordinate strategy for promoting both science and technology research and policy. Presidential Science Adviser Dr. Neal Lane and the Australian Minister of Industry, Science and Resources issued a Joint Statement on Scientific and Technological Cooperation in Canberra on November 1 to signal the two countries' intention to negotiate a new S&T agreement. The Australian government agreed separately to conduct a survey of all ongoing CIP R&D and meet over the next year to identify areas for possible joint projects.

Conclusion

The globalization of technology is a dominant force shaping today's world economy. In fact, calls for a more activist Federal technology policy stem in large part from the recognition of this shift in the geographic distribution of the world's technological capabilities. What is not always noted, however, is that the very process of globalization calls into question the notion that technologies, industries, or even corporations have distinctive nationalities. It is impossible for any country to achieve its national science and technology objectives in isolation from other countries. Increasingly, the development of many high-payoff technologies is a high-risk, and costly venture, which exceeds the capacity and capabilities of individual firms, and even of countries. International S&T relations have become an integral part of overall U.S. foreign policy and play a vital role in meeting the challenges of infrastructure protection.